AMENDMENTS TO THE CLAIMS

LISTING OF CLAIMS

Claims 1-12 (canceled, without prejudice)

Claim 13 (amended): A method for operating a computer security system comprising:

providing a badge ~~having a data processing system~~ to an individual, the badge comprising:

a non-volatile memory;

~~a volatile memory;~~

~~a transceiver for sending and receiving signals utilized by said badge;~~ and

an attachment sensor for detecting the removal of said badge from an individual, said attachment sensor causing information stored in said volatile memory to be rendered unreadable when said attachment sensor detects said removal;

~~providing an identity verification system for authenticating identity of the individual~~determining whether the individual possessing the badge belongs to a set of authorized individuals, said determining comprising evaluating the individual, separate from the badge, using an identity verification system; and

~~subsequently causing an administrative device to load information in said volatile memory of said badge~~ in response to said identity verification system determining the individual belongs to the set of authorized individuals~~authenticating the individual~~, subsequently causing an administrative device to load information into said volatile memory of said badge, said information specifying the level of access to said computer system to which the individual is entitled.

Claim 14 (previously presented): The method of Claim 13 wherein said causing the administrative device to load information comprises:

establishing a secure communication channel between the administrative device and that badge by encrypting signals sent and received by said transceivers in the administrative device and that badge; and

sending said information on said secure communication channel.

Claim 15 (previously presented): The method of Claim 13 wherein said identity verification system compares the retina of the individual with data derived from a previous measurement on the individual's retina.

Claim 16 (previously presented): The method of Claim 13 wherein said information loaded by the administrative device into the badge includes a code that is periodically changed.

Claim 17 (amended): A security badge comprising:

a non-volatile memory;

a volatile memory;

a transceiver for sending and receiving signals utilized by said badge; and

an attachment sensor for detecting the removal of said badge from an individual, said attachment sensor causing information stored in said volatile memory to be rendered unreadable when said attachment sensor detects said removal;

wherein an administrative device may load information in said volatile memory of said badge in response to and subsequent to an identity verification system authenticating an individual maintaining said badge as belonging to a set of authorized individuals, said information specifying the level of access to a ~~computer system~~ client computer to which the individual is entitled.

Claim 18 (previously presented): The ~~method~~ security badge of Claim 17 wherein said information loaded by the administrative device into the badge includes a code that is periodically changed.

Claim 19 (previously presented):   The ~~method~~ security badge of Claim 17 wherein
the administrative device loading information comprises:

establishing a secure communication channel between the administrative
device and that badge by encrypting signals sent and received by said transceiver in
the badge; and

sending said information on said secure communication channel.

Claim 20 (new)   A method for operating a computer system comprising an
administrative computer, said method comprising:

providing a badge to an individual, said badge having a volatile memory, a
transceiver for sending and receiving signals, and an attachment sensor for detecting
the removal of said badge from that individual, said attachment sensor causing
information stored in said volatile memory to be rendered unreadable when said
attachment sensor detects said removal;

providing the administrative computer with a transceiver for communicating
with the badge and an identity verification system for determining whether the
individual, distinct from the badge, belongs to a set of authorized individuals; and

upon determining that the individual possessing the badge personally belongs
to the set of authorized individuals, subsequently causing the administrative computer
to load information in said volatile memory of said badge, said information specifying
the level of access to said computer system to which the individual is entitled.

Claim 21 (new):   The method of Claim 20 wherein said subsequently causing the
administrative computer to load information comprises:

establishing a secure communication channel between the administrative
computer and the badge by encrypting signals sent and received by said transceivers
in the administrative computer and that badge; and

sending said information on said secure communication channel.

Claim 22 (new): The method of Claim 20 wherein said identity verification system compares the retina of the individual with data derived from a previous measurement on the individual's retina.

Claim 23 (new): The method of Claim 20 wherein said identity verification system compares a finger print of the individual with data derived from a previous measurement on the individual's finger print.

Claim 24 (new): The method of Claim 20 wherein said identity verification system compares the voice of the individual with data derived from a previous measurement on the individual's voice.

Claim 25 (new): The method of Claim 20 wherein said identity verification system compares answers to queries posited to the individual with data previously provided by the individual.

Claim 26 (new): The method of Claim 20, wherein said computer system further comprises a client computer, the method further comprising:

providing the client computer with a transceiver for communicating with the badge possessed by the individual;

causing the client computer to verify authenticity of the badge separate from the individual by receiving data derived from the data stored in said volatile memory of the badge by the administrative computer; and

causing the client computer to provide the individual with access to said computer system, where level of access depends on the data stored in the badge.

Claim 27 (new): The method of Claim 26, wherein said computer system further comprises a client computer, and wherein the client computer periodically verifies presence of the individual by sending to and receiving signals from the badge.

Claim 28 (new): The method of Claim 27, wherein the client computer utilizes a first secure code to exchange data with the badge when verifying the authenticity of the badge.

Claim 29 (new):   The method of Claim 28, wherein the client computer utilizes a second secure code to verify the presence of that individual, said second secure code requiring less computational resources than said first secure code.

Claim 30 (new):   The method of Claim 29, wherein said second secure code depends on said first secure code and changes each time the client computer verifies the presence of the individual.

Claim 31 (new):   The method of Claim 30, wherein said information loaded by the administrative computer into the badge includes a code that is periodically changed.